Policy: 8075-4- Database Systems Standard
Section: Database Standards
Office/Department: Office of IT Application Support & Development

Reports To: Division of Information Technology
Contact: 404-631-1000

PURPOSE

The purpose of this standard is to ensure database integrity, high availability, optimum performance, and effective operations. All application projects are required to adhere to these standards. This standard is in effect for enterprise class database management systems only.

SCOPE

This policy applies to all Database Support and Data Warehouse personnel (including employees, contractors, vendors and other third parties) actively engaged in the support, deployment, or modification of any enterprise class database system. Exception to this standard must be approved by the Administrator of IT Applications.

RESPONSIBILITY

1. The Administrator of the Office of IT Applications is responsible for compliance with the standard, updates to the standard, and enforcing the standard.
2. The Database, Data Warehouse and Application Support Team Leaders are responsible for compliance with the standards and for reporting concerns to the IT application administrator.

DEFINITIONS

n/a

STANDARDS

A. Design Specification and Requirements

1. A high-availability strategy such as failover, mirroring, and/or the use of online backups must be used for databases that require 24 x 7 availability.
2. OLTP (Online Transaction Processing) data that is used by online users for mission-critical day-to-day operations and OLAP (Online Analytical Processing) data used for ad-hoc queries and decision support should be segregated into separate databases and/or servers.

3. Databases that have high availability and concurrency requirements, support high transaction rates, and share data across multiple departments and applications are good candidates for centralization. These types of databases require a great deal of operational and database administrative support.
4. All replicated data must be designed to be read-only. Updates must occur at the source where the data originates to promote data integrity and facilitate ease of data management. Replication of data must be based on requirements such as availability, security, performance, or decision support. Replication shall be used to:
    - ensure uninterrupted access to critical data
    - isolate production data from external users
    - facilitate load balancing through synchronization of distributed databases
5. Any new database implementation or migration of legacy data source to GDOT target data architecture shall use a GDOT approved relational DBMS, and support ANSI Standard SQL (currently SQL92), and shall also comply with ODBC and JDBC standards.
    - Nonstandard language features may be used only when the needed operation or function cannot reasonably be implemented with the standard features alone. This will require IT Application Administrator approval, and shall be documented in design documentation.
    - The use of standard features shall be favored over optional vendor-specific features to prevent being locked into a vendor-specific solution.
6. The source data that populates a data warehouse must be accurate. End users shall have read-only access to data warehouse.
7. Any updates to an authoritative source OLTP system will only be carried forward after the application of the governing business rules. Commercial off the Shelf (COTS) software shall be configurable to allow for data validation. To reduce the risk of inaccurate or misleading data and to reduce the need for data cleansing, data quality validations shall be built into new and existing application systems.
8. All systems should include an accurate data model, created by a cooperative effort between the Business Unit and Database Developers to ensure that the logical and physical designs satisfy the business requirements.
9. Purge criteria shall be established for all databases, and shall be in accordance with GDOT record retention schedules. Data that is no longer needed shall be purged or archived to a less expensive media in accordance with GDOT data retention requirements, policies, or historical significance.
10. Metadata with its security classification shall be captured and maintained for both OLTP and OLAP environments to facilitate data sharing within GDOT and among its business partners. Business process owners and developers, including contractors, are responsible for documenting elements stored in the database, and shall follow the GDOT metadata standards.

B. Production Specifications and Requirements

1. When implementing a data warehouse or data mart, a network assessment shall be done to determine the potential impact on the network.
2. Microsoft Access databases and other desktop or non-approved databases shall not be used to develop standalone applications. Microsoft Access shall not be used to support enterprise reporting. These types of systems are difficult to support and shall not be used to support critical business functions.
3. Production databases supporting mission-critical applications must be recoverable to a point-in-time and point-of-failure.

- Database transaction logging must always be active for mission-critical production applications. Database backup must be sent offsite weekly, at a minimum.
- A backup/recovery plan must be in place and tested at least twice a year to prevent loss of data due to application/software errors, or from hardware failures.
- Database backups shall be scheduled frequently enough to ensure optimum recovery times.

4. An internal auditing process shall be put in place to ensure that GDOT is in compliance with all security, privacy, and information dissemination laws. Database Administrators should work closely with security officers to ensure that information is stored, managed, accessed and secured in compliance with Federal and State privacy laws as well as other laws impacting GDOT program areas.
5. All platforms used for hosting mission-critical applications shall be fully supported by the vendor and provide optimum performance. DBMS vendors acknowledge these platforms as preferred or tier-1. Vendor support shall provide better access to the latest versions of products, timely patches, and to knowledgeable technical support on preferred/tier-1 platforms.
6. Database Backups for mission-critical applications shall be tested at least four times a year. An updated Disaster Recovery (DR) Plan shall be available that documents the operational procedures required for the recovery, including procedures for retrieving offsite copies of database backups. Backups cannot be assumed to be complete until they are tested. Database management team leader shall ensure that all DBAs understand the steps needed to perform a recovery / testing, and will insure minimal downtime when an actual recovery needs to be performed.
7. Databases for mission-critical applications shall be monitored proactively for capacity planning purposes and to maintain high availability. Statistics such as transaction rates, allocated extent size, system CPU, and archive log volume shall be included. A database shall never stop functioning for foreseeable events. Events such as file systems filling up, objects not able to allocate additional extents, and objects reaching max extents shall be actively monitored and a DBA notified, before the problem causes the database to halt.
8. Database permissions shall be granted at the minimum level required.
    - Limit the members of the System or Database Administrators role to trusted DBAs.
    - Create custom database roles, if required, for better control over permissions.
    - Application programs or interfaces shall never be given "sysadmin" / "sysdba" authority.
    - Default accounts shall be changed.
    - Production passwords shall be changed from test or development environments.
    - A process shall be put in place to monitor the activity of those with System or Database Administration authority.
9. Error logs and event logs for security-related alerts/errors shall be monitored, and notification shall be sent to database administrators for appropriate support task. The use of Intrusion Detection Systems (IDS), especially on mission-critical database servers, must be implemented. IDS can constantly analyze the inbound network traffic, look for trends and detect Denial-of-Service (DoS) attacks and port scans. IDS can be configured to alert the administrators upon detecting a particular trend.
10. DBAs shall remain current with the information on the latest service packs and security patches released by DBMS vendors. All the service packs and patches shall be carefully evaluated and applied according to vendor recommendations.
11. Application Capacity Planning must be done at least once a year to determine the impact on mission-critical

databases. This plan will enable System Administrators and management to accurately forecast future hardware/software capacity requirements. The plan shall address topics such as transaction rates, physical storage needs, software licensing, machine utilization, etc., and shall be updated periodically to anticipate future needs at 6 and 12 month intervals, or longer based on procurement lead time.

12. A process shall be established to regularly stress test mission-critical applications. The stress test will simulate anticipated normal and peak usage of the application and the impact on the infrastructure. The results of the test shall be reviewed by a performance team comprised of the application, database, network, and other technical support personnel responsible for performance issues.
13. Statistics related to normal database operations, networks and applications shall be collected and available for a minimum of 3 months. Having a baseline set of statistics encompassing server, database, and network and application utilization will prove to be invaluable, when problem issues arise.
14. A Change Management Process to coordinate and communicate infrastructure, application, and database related changes shall be put in place. Having a defined process for approval and notification provides overall coordination of activities and limits exposure to multiple simultaneous changes from occurring.
15. Database Management Systems and the Operating Systems that they run on shall be on version/release levels that are fully supported by the vendor.

References:

None.

History:

Copied to GDOT Publications v.02.00.00 on 2/29/2012
Created and made effective September 01, 2009 Reviewed: 5/5/2011
Created at 10/1/2009 2:28:50 PM by Karen Mack